PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 7/04, G07D 7/00, E05B 49/00

A1

(11) International Publication Number: **WO 97/27533**

(43) International Publication Date: 31 July 1997 (31.07.97)

(21) International Application Number: PCT/US96/14895

(22) International Filing Date: 16 September 1996 (16.09.96)

(30) Priority Data:
08/589,614 22 January 1996 (22.01.96) US

(71)(72) Applicant and Inventor: TESAR, Gerald, T. [US/US]; 1167 Peak Circle, Deltona, FL 32738 (US).

(74) Agent: LIVINGSTON, Edward, M.; 628 Ellen Drive, P.O. Box 1599, Winter Park, FL 32790 (US).

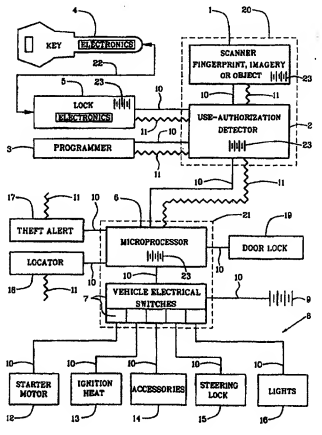
(81) Designated States: AU, BR, CA, CN, JP, KP, KR, MX, NO, PL, RU, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: VEHICLE SECURITY SYSTEM

(57) Abstract

A vehicle-security system has a use-authorization detector (2, 2A) with which vehicle-electrical systems (8, 12, 13, 14, 15, 16) are activated and deactivated separately from selection of desired vehicle-electrical systems for operational control. The use-authorization detector, vehicle-electrical switching (7) and related wiring (10) are positioned in design proximity and housed for inaccessibility to hot-wiring. An electronic key (4) is used to select activated vehicle-electrical systems through a matching electronic lock (5) that is separate from the use-authorization detector and positioned in design relationship to vehicle-steering controls. Electrical communication between the electronic lock and the use-authorization detector does not include wiring which could be hot-wired. Use-authorization indicia are programmably adjustable for long-term and temporary user authorization. Controller door-lock (19), locator (18) and theft-alert (17) features are optional.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic	SD	Sudan
CF	Central African Republic		of Korea	SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

VEHICLE SECURITY SYSTEM

Background of the Invention

This invention relates to vehicle-security systems and in particular to a vehicle security system with computerized control of electrical systems of vehicles to prevent vehicle theft or unauthorized use.

Various electronic and battery systems have been devised to operate in relation to an ignition switch of vehicles to prevent their theft or unauthorized use. None are known, however, to be owner-identifiable and owner-adaptable in a manner taught by this invention.

Examples of vehicle-security devices and methods that are different from this invention are described in the following patent documents. U.S. Patent Number 5,289,177, issued to Wake on February 22, 1994, taught a burglarproof key cylinder lock with a coded magnetic key. U.S. Patent Number 5,311,757, issued to Spahn on May 17, 1994, taught a key that was coded mechanically as well as electronically to activate mating components of an ignition switch of a vehicle. U.S. Patent Number 5,083,362, issued to Edgar et al on January 28, 1992, taught a method that employed mechanical swaging for construction of a key having a resistor pellet as an element of electronic control of an ignition system. U.S. Patent Number 5,003,801, issued to Stinar et al on April 2, 1991, described a key and lock assembly having an electronically coded circuit embedded in a handle of the key and connectors from the handle to contact points

outside of a keyhole. U.S. Patent Number 4,331,013, issued to Jaulmes on May 25, 1982, taught a key with magnets that operated a plurality of magnetic switches that functioned as tumblers in an ignition switch. U.S. Patent Number 4,789,859, issued to Clarkson et al on December 6, 1988, taught a lock system that was transitional between mechanical and electronic lock systems.

None of the known prior art prevents hot-wiring of vehicles sufficiently to prevent their professional theft or their unauthorized use. Instead, prior art of record mostly improves identification and rejection of unauthorized keys at vehicular positions where electrical wires are accessible for bypassing ignition switches. Consequently, there is still a high commercial volume of vehicle larceny. Criminal procedures have tended to keep pace with vehicle-security technology that is affordable to vehicle purchasers and compatible with the economics of vehicle maintenance.

Summary of the Invention

In light of a growing demand for improved protection against theft and unauthorized use of vehicles, objects of this invention are to provide a vehicle-security system which:

Prevents operation of electrical systems of a vehicle without design identification of an authorized user of the vehicle;

Has an electronic key system with which electrical operations of a vehicle are selected in addition to prevention of operation of the electrical systems of the vehicle without the design identification of the authorized user;

Positions a vehicular-electrical switch and related lead electrical wiring where inaccessible to hot-wiring and in design proximity to a user-identification means;

Provides a selection of user-identification means having different complexities and related costs for different types of vehicles, different preferences of users and different use conditions;

Provides means for long-term and temporary changing of identity for authorized use as desired by an owner or legitimate controller of a vehicle;

Provides means for theft notification to owners, to proper officials and to surrounding public as desired; and

Provides an optional means for controlling vehicle entry.

This invention accomplishes these and other objectives with a vehicle-security system having a use-authorization detector with which vehicle-electrical systems are activated and deactivated separately from selection of desired vehicle-electrical systems for operational control. The use-authorization detector, vehicle-electrical switching and related lead wiring are positioned in design proximity and housed for inaccessibility to hot-wiring. An electronic key is used to select

activated vehicle-electrical systems through a matching electronic lock that is separate from the use-authorization detector and positioned in design relationship to vehicle-steering controls. Electrical communication between the electronic lock and the use-authorization detector does not include lead wiring which could be hot-wired. Use-authorization indicia are programmably adjustable for long-term and temporary user authorization. Controlled vehicle-entry, vehicle location and theft-alert features are optional.

The above and other objects, features and advantages of the present invention should become even more readily apparent to those skilled in the art upon a reading of the following detailed description in conjunction with the drawings wherein there is shown and described illustrative embodiments of the invention.

Brief Description of Drawings

This invention is described by appended claims in relation to description of a preferred embodiment with reference to the following drawings which are described briefly as follows:

FIG. 1 is a schematic diagram of a comprehensive embodiment with select positioning of operative use-authorization, microprocessing and switching components; with electronic-key selection of engine-electrical systems; with optionally direct-wiring or radio-wave communication between use-authorization

detector and switching components; with optionally remote or vehicle-mounted controls; and with optional theft-alert, vehicle-locator and door-lock features;

FIG. 2 is a schematic diagram of a dashboard embodiment with optionally direct-wiring or radio-wave communication between a use-authorization detector and switching components; with electronic-key selection of engine-electrical systems; with optionally remote or vehicle-mounted controls; and with optional theft-alert, vehicle-locator and door-lock features;

FIG. 3 is a partially cutaway and partially schematic side view of a dashboard embodiment with direct wiring between vehicle-electrical switches and vehicle-electrical systems;

FIG. 4 is a partially cutaway and partially schematic side view of an embodiment with dashboard positioning of a use-authorization detector having radio-wave communication to a microprocessor and vehicle-electrical switches in an engine compartment where designedly inaccessible to hot-wiring of vehicle-electrical systems, and with optional remote control of use authorization and a door lock;

FIG. 5 is a side view of a designedly electronic ignition key having a single designedly electronic unit;

FIG. 6 is a partially cutaway side view of an electronic ignition lock operable by the **FIG. 5** key;

FIG. 7 is a partially cutaway end view of the **FIG. 6** electronic ignition lock;

FIG. 8 is a side view of a designedly electronic ignition key having a plurality of designedly electronic units that are juxtaposed sequentially;

FIG. 9 is a side view of an electronic ignition lock operable by the **FIG. 8** key;

FIG. 10 is a side view of a designedly electronic ignition key having a plurality of designedly electronic units that are separated;

FIG. 11 is a partially cutaway side view of a **FIG. 8** key in a **FIG. 9** ignition lock having optionally direct-wiring or radio-wave communication of selection of vehicle-electrical systems for operation;

FIG. 12 is a scanner in optional combination with a programmer of use indicia and having optionally direct-wiring or radio-wave communication of indicia of use authorization;

FIG. 13 is a top view of an elongate programmer of use indicia such as multiple fingers or other use indicia and having optionally direct-wiring or radio-wave communication of indicia of use authorization;

FIG. 14 is a front elevation view of the **FIG. 13** illustration; and

FIG. 15 is a side elevation view of the **FIG. 13** illustration.

Description of Preferred Embodiment

Reference is made first to **FIG. 1,** which is a schematic diagram of a comprehensive embodiment with optional features. A scanner **1** communicates indicia of use authorization to a use-authorization detector **2** which is programmable with a programmer **3** to detect programmed fingerprint, imagery and/or object indicia of use authorization. An electronic key **4** has designedly operable relationship to an electronic lock **5** with which a microprocessor **6** is employed to select vehicle-electrical switches **7** for electrical operation of vehicle-electrical systems **8** which are powered by a source **9** of vehicle electricity such as a battery.

A selection of direct-wiring **10** communication and/or radio-wave **11** communication can be employed between the scanner **1** and the use-authorization detector **2**, between the use-authorization detector **2** and the microprocessor **6**, between the electronic lock **5** and the use-authorization detector **2**, and between the programmer **3** and the use-authorization detector **2**. Direct wiring **10** is employed for electrical communication between the source **9** of vehicle electricity and the vehicle-electrical switches **7**, between the vehicle-electrical switches **7** and the vehicle-electrical systems **8**, and between the microprocessor **6** and the vehicle-electrical switches **7**.

Vehicle-electrical systems **8** which can be selected with the electronic key **4** positioned in the electronic lock **5** for operation in accordance with vehicle design can include such electrical systems as a starter motor **12**; ignition heat **13** with spark plugs or various forms of heat-assistance glow plugs; accessories **14**; a steering lock **15**; and lights **16**. Also operable through the microprocessor **6** as programmed can be a theft alert **17** to notify applicable protection authorities, the owner or possible people in a vicinity of the vehicle that theft of the vehicle is being attempted. Communication to the applicable protection authorities is preferably by radio wave **11** communication. A locator **18** to assist in finding a vehicle that has been used without authorization also can be activated by the microprocessor **6** to send out location indicia with radio-wave **11** communication. The same locator **18** can be employed as programmed also to operate audio or visual signals from a forgotten location of the vehicle in a large parking lot or from a wave-muffling location where the vehicle may be hidden by a thief. Further yet, a door lock **19** can be operated as programmed by an authorized user to aid quick entry into the vehicle for security and/or convenience of an authorized user.

A primary objective is to position the vehicle-electrical switches **7** where they cannot be hot-wired and using the electronic ignition key **4** only to select activated vehicle-electrical systems **8**. No wiring to vehicle-electrical systems **8**

or to vehicle-electrical switches **7** is positioned at the electronic lock **5** or proximate a steering column where accessible to a thief.

A select use area **20** is indicated by dashed lines encompassing the scanner **1** and the use-authorization detector **2**. The scanner **1** can be remote from the use-authorization detector **2** and/or portable as designed. The use-authorization detector **2** can be separated from or attached to the microprocessor **6**. Housing **21** for inaccessibility to hot-wiring is indicated by dashed lines surrounding the microprocessor **6** and the vehicle-electrical switches **7**.

Positioning of the electronic key **4** in and out of the electronic lock **5** is represented by a two-way key arrow **22**.

A separate electrical source **23** can be provided for operating the scanner **1**, the use-authorization detector **2**, the electronic lock **5**, and the microprocessor **6** to prevent dependence on electrical leads to the source **9** of vehicle electricity which could be disconnected or variously incapacitated.

In **FIG. 2**, a dashboard embodiment diagramed is more compact with the scanner **1** and the use-authorization detector **2** in a select use area **20** that is a housing positioned proximate passenger-compartment side of a dashboard **24**. Preferably the microprocessor **6** is positioned opposite the select use area **20** in a housing **21** that is designed for unauthorized accessibility and positioned

proximate an engine-compartment side of the dashboard **24** for inaccessibility to hot-wiring of the vehicle.

All direct wiring **10** is preferred for this embodiment. Electrical communication **11** described in relation to **FIG. 1** could be used, however, between the electronic lock **5** and the use-authorization detector **2**. Wiring **10** from the use-authorization detector **2** to the microprocessor **6** is routed through the dashboard **24**. Optionally, the dashboard **24** can be positioned between the scanner **1** and the use-authorization detector **2** with wiring **10** routed through the dashboard **24**. The scanner **1** is preferably an optical scanner which scans and reads authorized fingerprints as programmed by the programmer **3** for detection and communication to the use-authorization detector **2**.

The compact **FIG. 2** embodiment can be less expensive for some user preferences. It can, however, have a theft alert **17**, as described in relation to **FIG. 1**, without increasing its cost excessively for some user preferences.

In **FIG. 3**, a dashboard embodiment depicted is positioned in a car **25** with structural division between the scanner **1** and the use-authorization detector **2** proximate the dashboard **24**. The electronic lock **5** is positioned on a steering column **26**, but can be positioned variously in relation to the dashboard **24** and the steering column **26**. The vehicle-electrical switches **7** are projected into an engine compartment **27** where wiring **10** is directed to vehicle-electrical systems

8 that are positioned in design relationship to an engine 28. Positioning of the use-authorization detector 2 on the dashboard 24 can be proximate the steering column 26.

In this embodiment, a programmer 3 is assumed to be integrated with the use-authorization detector 2 for cost purposes. A door lock 19 operated by a scanner 2 can be undistinguishable from a conventional door lock. A housing 21 for inaccessibility to hot-wiring can be omitted for this embodiment if engine-compartment positioning is sufficiently protective. A secure housing 21 is preferred, however, for protection against possibly ill-intentioned mechanics during repair, maintenance and servicing.

In FIG. 4, a comprehensive embodiment with select optional features has a use-authorization detector 2 positioned on a dashboard 24 where it is separate from the microprocessor 6 and the vehicle-electrical switches 7 which are positioned in the engine compartment 27. A scanner 1 and a programmer 3 can be positioned on or separately from the use-authorization detector 2. The microprocessor 6 is operated through radio-wave 11 communication from the use-authorization detector 2. Communication from the electronic lock 5 to the use-authorization detector 2 can be either by direct wire 10 or by radio wave 11 as described in relation to FIG. 1.

In addition to or optionally to positioning the scanner **1** on a dashboard **24** in combination with a use-authorization detector **2** and a programmer **3**, a scanner **1** can be positioned separately and portable with a transmitter **29** for operation of the use-authorization detector **2** by radio wave **11**. Also in addition to or optionally to positioning the use-authorization detector **2** on a dashboard **24**, an outside use-authorization detector **2A** can be positioned on a design outside location, such as near a door lock **19**, The theft alert **17**, locator **18** and door lock **19** then can be operated also through the microprocessor **6** as described in relation to **FIG. 1**. Communication from the theft alert **17** can be through radio wave **11** from a radio antenna **30**. The locator **18** can be a pulsating LED or other light and/or an audio emitter positioned on a tip of the radio antenna **30** or other suitable place.

Referring to **FIGS. 5-11**, the electronic key **4** is preferably flat or un-slotted regardless of flatness, roundness or other physical configuration that is designedly uniform to obviate need for key perforations and matching lock perforations. Instead, a single electronic key chip **31** as shown in **FIG. 5**, a design plurality of electronic key chips **32** arranged consecutively as shown in **FIGS. 8** and **11** or separated electronic lock chips **33** as shown in **FIG. 10** can be employed for respectively matching electronic locks **5** as shown in **FIGS. 6, 7, 9** and **11.**

In **FIG. 6**, correspondingly configured long electronic lock chips **33** are positioned arcuately as shown in **FIG. 7** to match rotational positioning of the electronic key **4** in a keyhole **34** for selection of separate vehicle-electrical switches **7** as described in relation to **FIG. 1**.

In **FIG. 9**, there is a separate electronic lock chip **35** for each of a design plurality of vehicle-electrical switches **7**, described in relation to **FIG. 1**, which are selected by a matching design plurality of electronic key chips **32** shown in **FIG. 8**. In **FIG. 11**, the design plurality of electronic key chips **32** are shown in open-circuit relationship to the design plurality of electronic lock chips **35**. Lock-chip lead lines **36** are routed through a lock circuitry **37** for communication of selection data through a lock communicator **38** with either direct wiring **10** or radio wave **11**. A separate electrical source **23** is in electrical communication with the lock communicator **38** for communication means which require electrical current. In **FIG. 10**, the plurality of electronic key chips **32** are separated for particular design preferences.

A variety of arrangements of designedly coded electronic key chips **31** and **32** in relation to electronic lock chips **33** and **35** have been designed and more yet are foreseeable. Specialized magnets also are foreseeable as electronic chips or for use in combination with electronic chips. Magnets can be employed to activate switches that coded chips select for activation.

Referring to **FIG. 12**, a scanner **1** which is portable or attached to a use-authorization detector **2** can have a scanner screen **39** proximate a programmer **3** with a programmer switch **40** that allows a user with an authorized fingerprint, image or object to activate the scanner **1** or to alter programming in accordance with switching design. Messages of operation or alteration of operation then can be transmitted by directing wiring **10** or radio wave **11** in accordance with a particular design.

Referring to **FIGS. 13-15**, a separate programmable scanner **41** can be provided with an elongate scanner screen **42** for scanning all fingerprints on the fingers of one hand. The elongate scanner screen **42** can be used also for scanning images such as written or graphic representations or for scanning objects. A program-selection knob **43** can be rotated or otherwise indexed to computer components for altering long-range indicia of use authorization, for altering temporary indicia of use authorization or for using existing use authorization. Indexing to computer components for desired operation can be indicated by a selection point **44** on the program-selection knob **43** which points to program-selection indicia **45**.

This vehicle-security system teaches a unique working relationship of electronic, electrical, and mechanical parts, some of which are specially

designed and some of which are known separately. Various selections and modifications of these parts are foreseeable within the scope of this invention.

A new and useful vehicle-security system having been described, all such modifications, adaptations, substitutions of equivalents, combinations of parts, mathematical possibilities of combinations of parts, pluralities of parts, applications and forms thereof as described and foreseeable by the following claims are included in this invention.

CLAIMS

Having thus described my invention, I claim:

1. A vehicle-security system comprising:

a use-authorization detector having activation-deactivation-switching relationship between design vehicle-electrical systems and a source of vehicle electricity;

an electronic key having operable relationship to an electronic lock which has selection relationship to vehicle-electrical systems which are activated by the use-authorization detector;

the use-authorization detector, vehicle-electrical switching and related lead wiring between select vehicle-electrical systems and the source of vehicle electricity being positioned in design interworking relationship and housed for inaccessibility to hot-wiring of the select vehicle-electrical systems;

the electronic lock being separate from the use-authorization detector and positioned in design relationship to vehicle-steering controls; and

designedly electrical-related communication between the electronic lock and the use-authorization detector for selection of vehicle-electrical systems which are activated by the use-authorization detector for design operation.

2. A vehicle-security system as described in claim 1 wherein:

the use-authorization detector has an optical scanner with a capability of recognizing design criteria of use authorization and communicating acceptableness of the design criteria of use authorization through design communication means to a microprocessor with which circuitry between the source of vehicle electricity and design vehicle-electrical systems is switched in accordance with determination of use authorization by the use-authorization detector.

3. A vehicle-security system as described in claim 2 wherein:

the design criteria of use authorization which the optical scanner has a capability of recognizing is a fingerprint.

4. A vehicle-security system as described in claim 3 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned opposite a wall of a switch container from the use-authorization detector where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

5. A vehicle-security system as described in claim 3 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

6. A vehicle-security system as described in claim 3 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

7. A vehicle-security system as described in claim 3 wherein:

the use-authorization detector is positioned designedly proximate a steering column of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

8. A vehicle-security system as described in claim 3 wherein:

an outside use-authorization detector is positioned proximate a design portion of an outside periphery of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

9. A vehicle-security system as described in claim 8 wherein:

the design portion of the outside periphery of the vehicle is in design proximity to a handle to a door of the vehicle.

10. A vehicle-security system as described in claim 3 wherein:

a scanner is positioned on a portable transmitter;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

11. A vehicle-security system as described in claim 1 wherein:

design relationship to vehicle-steering controls where the electronic lock is positioned is on a steering column.

12. A vehicle-security system as described in claim 11 wherein:

the designedly electrical-related communication between the electronic lock and the use-authorization detector for selection of activated vehicle systems is with direct wiring.

13. A vehicle-security system as described in claim 11 wherein:

the designedly electrical-related communication between the electronic lock and the use-authorization detector for selection of activated vehicle systems is with radio wave.

14. A vehicle-security system as described in claim 1 wherein:

design relationship to vehicle-steering controls where the electronic lock is positioned is designedly proximate a dashboard.

15. A vehicle-security system as described in claim 14 wherein:

the designedly electrical-related communication between the electronic lock and the use-authorization detector for selection of activated vehicle systems is with direct wiring.

16. A vehicle-security system as described in claim 14 wherein:

the designedly electrical-related communication between the electronic lock and the use-authorization detector for selection of activated vehicle systems is with radio wave.

17. A vehicle-security system as described in claim 1 wherein:

the electronic key has a physical shape that is designedly uniform to other electronic keys using the vehicle-security system.

18. A vehicle-security system as described in claim 17 wherein:

operable relationship of the electronic key to the electronic lock is with at least one electronic key chip having communicative relationship to at least one electronic lock chip.

19. A vehicle-security system as described in claim 18 wherein:

the at-least-one electronic lock chip is a separate electronic lock chip for each of a design plurality of vehicle-electrical switches with which the at-least-one lock chip has design electronic communication; and

the electronic key is positional in the electronic lock to communicative relationship of the at-least-one electronic key chip with the at-

least-one electronic lock chip for activation-deactivation switching between desired vehicle-electrical systems and the source of vehicle electricity.

20. A vehicle-security system as described in claim 18 wherein:

the at-least-one electronic key chip is a design plurality of electronic key chips;

the at-least-one electronic lock chips is a design plurality of electronic lock chips;

select electronic key chips of the design plurality of electronic key chips have electronically communicative relationship with select electronic lock chips of the design plurality of electronic lock chips; and

the electronic key is positional selectively in the electronic lock to communicative relationship of the at-least-one electronic key chip with the at-least-one electronic lock chip for activation-deactivation switching between desired design vehicle-electrical systems and the source of vehicle electricity.

21. A vehicle-security system as described in claim 1 wherein:

the design vehicle-electrical systems include a starter motor.

22. A vehicle-security system as described in claim 21 wherein:

the design vehicle-electrical systems include an ignition-heat system.

23. A vehicle-security system as described in claim 22 wherein:

the design vehicle-electrical systems include a steering-lock system.

24. A vehicle-security system as described in claim 2 wherein:

the design criteria of use authorization which the optical scanner has a capability of recognizing is a design selection of fingerprint, physical imagery and physical objects.

25. A vehicle-security system as described in claim 24 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned opposite a wall of a switch container from the use-authorization detector where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

26. A vehicle-security system as described in claim 24 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

27. A vehicle-security system as described in claim 24 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

28. A vehicle-security system as described in claim 24 wherein:

the use-authorization detector is positional remotely from the microprocessor;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

29. A vehicle-security system as described in claim 3 wherein:

the use-authorization detector is positional remotely from the microprocessor;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

30. A vehicle-security system as described in claim 1 and further comprising:

a detection programmer having computer-programming relationship to the use-authorization detector.

31. A vehicle-security system as described in claim 30 wherein:

the detection programmer has a long-term detection assimilator that is operable in relation to long-term objectives for recognizing design criteria of use authorization.

32. A vehicle-security system as described in claim 31 wherein:

the detection programmer has a short-term detection assimilator that is operable in relation to temporary objectives for recognizing design criteria of use authorization.

33. A vehicle-security system as described in claim 2 wherein:

the design criteria of use authorization which the optical scanner has a capability of recognizing is a design combination of fingerprint, physical imagery and physical objects.

34. A vehicle-security system as described in claim 33 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned opposite a wall of a switch container from the use-authorization detector where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

35. A vehicle-security system as described in claim 33 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is direct wiring.

36. A vehicle-security system as described in claim 33 wherein:

the use-authorization detector is positioned proximate a dashboard of a vehicle;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

37. A vehicle-security system as described in claim 33 wherein:

the use-authorization detector is positional remotely from the microprocessor;

the vehicle-electrical switching and related lead wiring are positioned proximate an engine compartment of the vehicle where designedly inaccessible to hot-wiring of vehicle-electrical systems; and

the design communication means from the use-authorization detector to the microprocessor is with radio wave.

38. A vehicle-security system as described in claim 1 and further comprising:

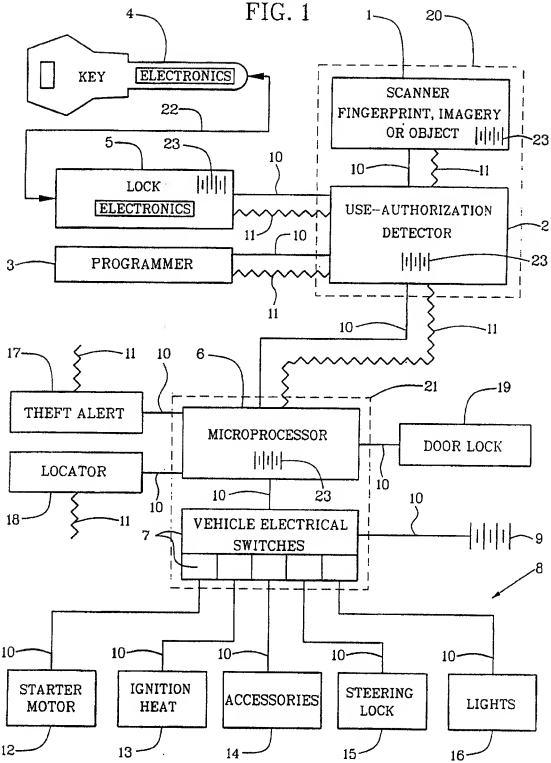
a theft-alert communicator in designedly operative relationship to the use-authorization detector in response to positioning of specific theft indicia in design proximity to the use-authorization detector.

39. A vehicle-security system as described in claim 1 and further comprising:

a theft-alert communicator in designedly operative relationship to the electronic lock in response to positioning of a theft-indicia key in the electronic lock.

1/6

FIG. 1


KEY
ELECTRONICS
SCANNER
FINGERPRINT, IMAGERY
OR OBJECT
LOCK
ELECTRONICS
USE-AUTHORIZATION
DETECTOR
PROGRAMMER
THEFT ALERT
MICROPROCESSOR
DOOR LOCK
LOCATOR
VEHICLE ELECTRICAL
SWITCHES
STARTER
MOTOR
IGNITION
HEAT
ACCESSORIES
STEERING
LOCK
LIGHTS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

2/6

FIG. 2

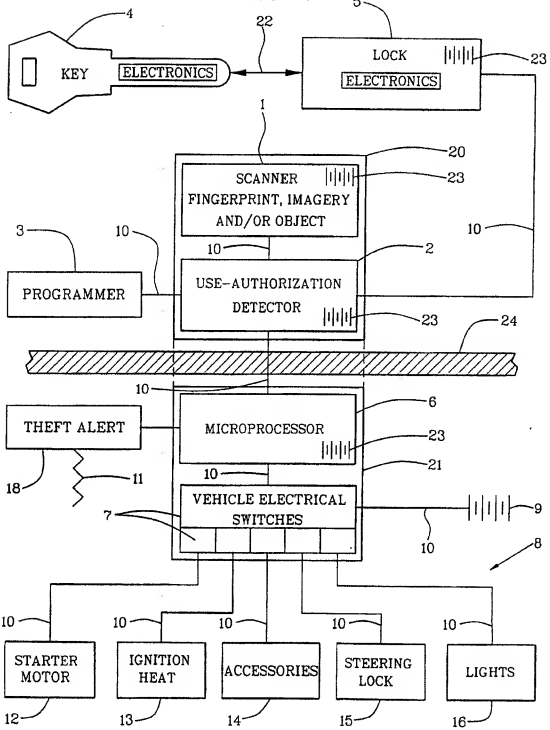
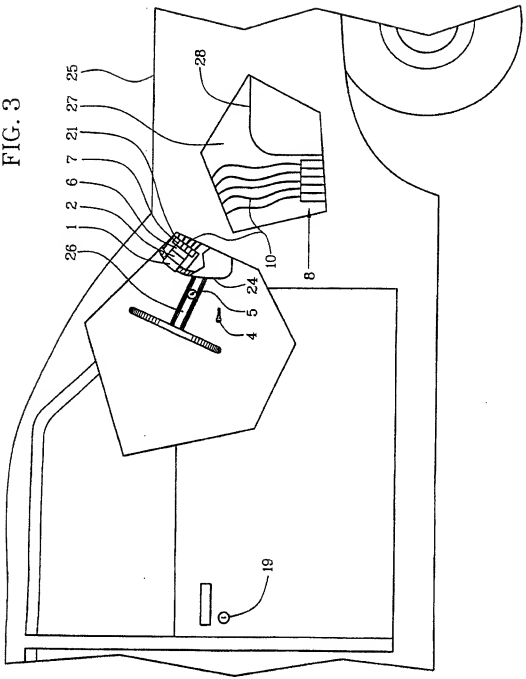

4
22
5
KEY
ELECTRONICS
LOCK
ELECTRONICS
23
1
20
SCANNER
FINGERPRINT, IMAGERY
AND/OR OBJECT
23
3
10
10
10
2
10
PROGRAMMER
USE-AUTHORIZATION
DETECTOR
23
24
10
6
THEFT ALERT
MICROPROCESSOR
23
18
11
10
21
VEHICLE ELECTRICAL
SWITCHES
9
7
10
8
10
10
10
10
10
STARTER
MOTOR
IGNITION
HEAT
ACCESSORIES
STEERING
LOCK
LIGHTS
12
13
14
15
16

FIG. 3



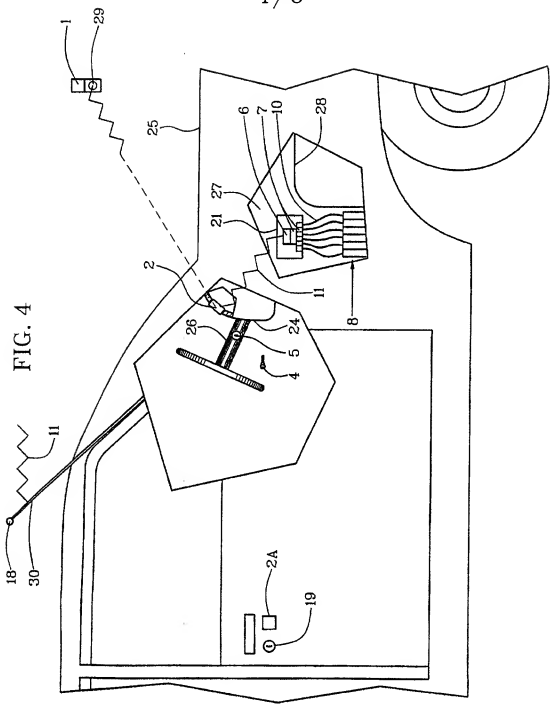


FIG. 4

FIG. 5

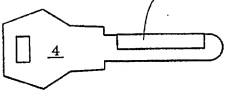


FIG. 6

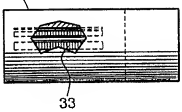


FIG. 7

FIG. 8

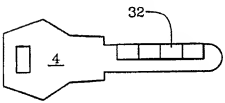


FIG. 9

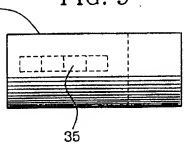


FIG. 10

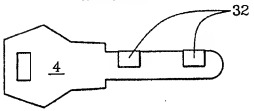


FIG. 11

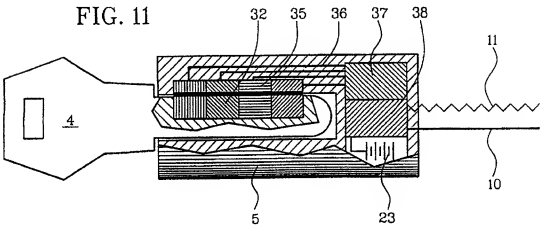


FIG. 12

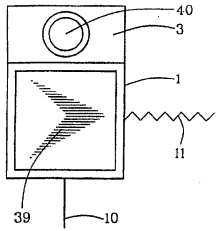


FIG. 13

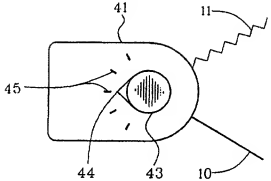


FIG. 14

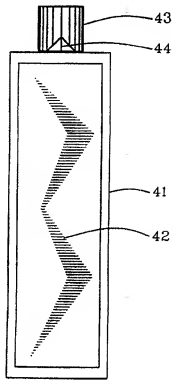
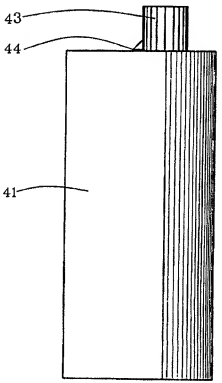


FIG. 15



INTERNATIONAL SEARCH REPORT

Inte ational application No.
PCT/US96/14895

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 7/04; G07D 7/00; E05B 49/00
US CL :340/825.31, 825.34; 70/278
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/825.30, 825.31, 825.32, 825.34; 70/277, 278; 382/124

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 4,189,712 (LEMELSON) 19 FEBRUARY 1980, ABSTRACT, FIGS 1 AND 14, COL. 1, LINES 6-20 AND 62-	1-2, 14-18, 21
---	66, COL. 3, LINE 23- COL. 4, LINE22, COL. 13, LINES 20-	--- 3-13,19-20,22-
Y	34, COL. 18, LINES 11-44.	39
Y	US, A, 5,337,043 (GOKCEBAY) 09 AUGUST 1994, ABSTRACT, FIG. 5, COL. 9, LINE 37- COL. 10, LINE 10.	3-13, 19-20, 22-39
A	US, A, 4,712,103 (GOTANDA) 08 DECEMBER 1987, ABSTRACT.	3
A	US, A, 5,311,757 (SPAHN) 17 MAY 1994, ABSTRACT.	1
A	US, A, 5,289,177 (WAKE) 22 FEBRUARY 1994, ABSTRACT.	1

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
31 DECEMBER 1996	08 MAY 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer EDWARD MERZ
Facsimile No. (703) 305-3603	Telephone No. (703) 305-4869

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

Inte..national application No.
PCT/US96/14895

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 5,083,362 (EDGAR ET AL.) 28 JUNE 1992, ABSTRACT.	1
A	US, A, 5,003,801 (STINAR ET AL.) 02 APRIL 1991, ABSTRACT.	1
A	US, A, 4,789,859 (CLARKSON ET AL.) 06 DECEMBER 1988, ABSTRACT.	1
A	US, A, 4,331,013 (JAULMES) 25 MAY 1982, ABSTRACT.	1
A	US, A, 4,347,545 (WEISHAUPT ET AL.) 31 AUGUST 1982. ABSTRACT.	1
A	US, A, 4,050,063 (SCHULL) 20 SEPTEMBER 1977, ABSTRACT.	1